CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A method of tracking-back a single malicious data packet in a connection-oriented communication network including a network node comprising a plurality of router interfaces, the method comprising the steps of:

a) for a given time window of a predetermined length~~(*Time Period*) extending over a configurable time period~~, computing a flow identifier that uniquely identifies ~~(*FlowId*) for uniquely identifying~~ a given flow seen by a respective router interface at said ~~(*Incoming Link*) at a~~ network node;

b) inserting said flow identifier ~~*FlowId*~~ into a data structure storing flow identifiers computed at said respective router interface during said time window~~associated to said Time Period and said *Incoming Link*, available at said network node~~;

c) storing said data structure in a searchable repository at said network node;

d) repeating steps a) to c) for a plurality of successive time windows, wherein each router interface stores a separate data structure for each time window~~next *Time Period* and for each router interface at said network node, for all packets seen at respective router interfaces over successive time windows, for populating said data repository with a plurality of data structures, each associated to a respective time period and a one of said respective router interfaces~~;

e) determining an arrival time window including a ~~the~~ time of arrival ~~X~~ of said single malicious packet at said network node, and computing a flow identifier ~~*FlowId*~~ for said single malicious packet; and

f) identifying said router interface ~~*Incoming Link*~~ for said single malicious packet by searching for the flow identifier ~~*FlowId*~~ of said single malicious packet in all data structures stored at said network node that contain data for said arrival time window~~for said network node that cover the time of arrival X~~.

2. (Canceled)

3. (Previously Presented) The method of claim 1, further comprising tracing-back hop by hop the source of said single packet from said router, by performing steps e) and f) for each network node along the path of said single malicious packet.

4. (Currently Amended) The method of claim 1, wherein step a) is based on a flow definition adopted for said network.

5. (Original) The method of claim 1, wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow.

6. (Original) The method of claim 1, wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow and an incoming interface identification parameter.

7. (Original) The method of claim 1, wherein step a) comprises applying a specified function to one or more characteristics of each packet.

8. (Original) The method of claim 1, wherein step a) comprises applying a specified function to one or more characteristics of each packet received in said flow and an incoming interface identification parameter.

9. (Original) The method of claim 1, wherein said data structure is a hash table based on a Bloom filter.

10. (Original) The method of claim 1, wherein said searchable repository is maintained for each router interface at said network node.

11. (Original) The method of claim 10, wherein said searchable repository stores all said data structures for all router interfaces at said network node.

12. (Original) The method of claim 1, wherein said searchable database is a centralized searchable repository maintained for said network.

13. (Currently Amended) A method of tracking-back a single malicious data packet in a connection-oriented communication network including a network node comprising a plurality of router interfaces, the method comprising the steps of:

a) for a given time window of a predetermined length~~(*Time Period*) extending over a configurable time period~~, computing a flow identifier that uniquely identifies ~~(*FlowId*) for uniquely identifying~~ a given flow seen by a respective router interface at said ~~(*Incoming Link*) at~~ a network node based on a flow characterization parameter obtained from a flow management system;

b) inserting said flow identifier ~~*FlowId*~~ into a data structure storing flow identifiers computed at said respective router interface during said time window~~, associated to said *Time Period* and said *Incoming Link*, available at said network node~~;

c) storing said data structure in a database that is a centralized searchable repository;

d) repeating steps a) to c) for a plurality of successive time windows, wherein each router interface stores a separate data structure for each time windownext ~~*Time Period* and for each *Incoming link* at said network node, for all packets seen at respective router interfaces over successive time windows, for populating said data repository with a plurality of data structures, each associated to a respective time period and a one of said respective router interfaces~~; and

e) finding, in said searchable repository, the router interface ~~*Incoming Link*~~ for said single malicious packet by searching for a corresponding flow identifier in all data structures containing data for an arrival time window, wherein the arrival time window includes a time of arrival of said single malicious packet~~based on a *FlowId* and a time of arrival X of said single malicious packet~~.

14. (Currently Amended) A system for tracking-back a single malicious data packet in a connection-oriented communication, comprising:

means for computing a flow identifier that uniquely identifies ~~*FlowId* for uniquely identifying~~ a given flow seen by a router interface ~~*(Incoming Link)*~~ at a network node ~~over~~ during a given time window of a predetermined length~~period of time *(Time Period)* extending over a configurable time period~~;

means for inserting said flow identifier ~~*FlowId*~~ into a data structure storing flow identifiers computed at said router interface during said time window~~associated to said *Time Period*. and said *Incoming Link* available for said network node~~;

a database that is a centralized searchable repository for storing said data structure; and

a search engine for finding, in said searchable repository, the router interface ~~*Incoming Link*~~ for said single malicious packet by searching for a corresponding flow identifier in all data structures containing data for an arrival time window, wherein the arrival time window includes a time of arrival of said single malicious packet~~based on a *FlowId* and a time of arrival X of said malicious packet~~.

15. (Previously Presented) The system of claim 14 further comprising a flow-based monitoring system for tracking back hop-by-hop the source of said single malicious packet.

16. (Currently Amended) The system of claim 14, wherein ~~one said~~ a searchable repository is maintained for each interface at said network node.

17. (Currently Amended) The system of claim 14, wherein ~~one said~~ a searchable repository is maintained for said network node.

18. (Currently Amended) The system of claim 14, wherein said searchable repository is a centralized database maintained ~~maintained'~~ for said network.

19. (Original) The system of claim 14, further comprising a flow based monitoring system for providing a flow characterization parameter to said means for calculating.

20. (Original) The system of claim 14 further comprising a flow management system for generating a flow characterization parameter.

21. (Currently Amended) The system of claim 20, wherein said means for computing is a flow identifier ~~*Flowld*~~ calculator for computing said flow identifier from at least one of ~~*Flowld*~~

~~form one or more of~~ packet header fields, packet characterization parameters, and interface identification information.

22. (Currently Amended) The system of claim 20, wherein said means for computing is a flow identifier ~~*Flowld*~~ calculator for computing said flow identifier from ~~*Flowld form*~~ packet header information.